REMARKS

The Examiner is thanked for the performance of a thorough search. Claims 1, 5, 9 and 13 have been amended as indicated herein. Hence, Claims 1-19 are pending in the application. It is respectfully submitted that none of the claim amendments add any new matter to this application. Furthermore, the claim amendments have been made solely to improve readability and clarity of the claims and not to overcome any prior art cited in the Office Action. All issues raised in the Office Action mailed December 10, 1998 are addressed hereinafter.

OBJECTION TO DRAWINGS

The drawings have been objected to on the ground that the margins are not acceptable as detailed in the Notice of Draftpersons Patent Drawing Review and correction has been requested. It is respectfully submitted that the drawings as filed with the application are suitable for examination purposes. Therefore, Applicant respectfully requests that the existing drawings be used for examination purposes. After the application has been allowed, new formal drawings correcting the deficiencies specified in the Notice of Draftpersons Drawing Review will be submitted.

REJECTION OF CLAIMS 1, 2, 5, 6, 13 AND 14 UNDER 35 U.S.C. §103(a)

Claims 1, 2, 5, 6, 13 and 14 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon et al.*, ("*Gillon*") U.S. Patent No. 5,838,927 in view of *Elgamal et al.*, ("*Elgamal*") U.S. Patent No. 5,657,390. It is respectfully submitted that Claims 1, 2, 5, 6, 13 and 14 are not unpatentable over *Gillon* in view of *Elgamal* based upon the teachings of *Gillon* and *Elgamal* as described hereinafter.

CLAIM 1

Claim 1 recites a method "for providing communication protocol-independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, where in the first network node and the second

network node each support at least one common communication protocol." Claim 1 requires the steps of:

"a) establishing a communication channel between the first network node and the second network node;
b) establishing a first stream between the first process and the communication channel;
c) establishing a second stream between the second process and the communication channel;
d) encrypting data to be transmitted between the first and second processes, the encrypting of the data being independent of the at least one communication protocol supported by the first and second network nodes;
e) writing the encrypted data to the first stream;
f) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol supported by the first and second network nodes;
g) reading the encrypted data from the second stream; and
h) decrypting the encrypted data to obtain decrypted data which is identical to the data on the first network node before the data was encrypted."

The invention recited in Claim 1 addresses the problem of how to provide layer-independent secure communications in a multi-layered communications network. Specifically, Claim 1 requires the steps of "d) encrypting data to be transmitted between the first and second processes, **the encrypting of the data being independent of the at least one communication protocol** supported by the first and second network nodes" and "f) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol supported by the first and second network nodes." According to steps d) and f), the data transmitted between the first and second processes is encrypted independent of the communication protocol used to transmit the data between the first and second network nodes. This allows decryption to be performed independent of the communication protocol and is therefore much more flexible than approaches that encrypt and decrypt using specific communication protocols or "layers".

Gillon and *Elgamal* do not teach or suggest, alone or in combination, a method for providing communication protocol-independent security that requires this step. *Gillon* describes an approach for compressing a continuous, indistinct data stream that involves examining a data stream to determine whether the data stream is compressible. If so, then the data stream is

attached to a compression stream and compression is performed to generate a compressed data stream that is transmitted continuously as it is generated.

The Office Action states that step d) of Claim 1 is described in *Gillon* at Col. 5, lines 60-67 and Col. 7, lines 4-15. However, at those locations *Gillon* does not describe how the encryption of a data stream is performed. More importantly, *Gillon* does not teach or suggest encrypting a data stream independent of a communication protocol supported by a network node on which a process resides. The text at Col. 5, lines 60-67 describes that when a data stream does not include a header, a file extension of the retrieved data is examined to determine what type of data may be found in the file. The text at Col. 7, lines 4-15 describes determining whether data is compressible by examining the header of the data and if so, attaching the data stream to a compression stream or any other type of stream such as an encryption stream. The compression stream and other streams are then attached to a right stream which is sent to the client.

Elgamal describes an approach for encrypting and decrypting information transferred over a network between a client application and a server application. A sockets application program interface is bound to a security protocol which is layered between an application layer and a transport layer. Since the security protocol is layered between an application layer and a transport layer, decryption must occur at or above the transport layer and is therefore dependent upon the transport layer communication protocol.

Since *Gillon* and *Elgamal* do not teach or suggest, alone or in combination, a method for providing communication protocol-independent security for data by encrypting the data **independent** of a communication protocol, it is respectfully submitted that Claim 1 is not unpatentable over *Gillon* in view of *Elgamal*. Therefore, the reconsideration and withdrawal of the rejection of Claim 1 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* is respectfully requested.

CLAIMS 2, 5, 6, 13 AND 14

Claims 5 and 13 are directed to a computer-readable medium and a computer data signal, respectively, that recite similar limitations to Claim 1. Therefore, it is respectfully submitted that Claims 5 and 13 are not unpatentable over *Gillon* in view of *Elgamal* for the reasons stated herein in support of Claim 1.

Claims 2, 6 and 14 depend from Claims 1, 5 and 13 and include all the limitations of Claims 1, 5 and 13. Therefore, it is respectfully submitted that Claims 2, 6 and 14 are not unpatentable over *Gillon* in view of *Elgamal* for the reasons stated herein in support of Claims 1, 5 and 13. Accordingly, the reconsideration and withdrawal of the rejection of Claims 2, 5, 6, 13 and 14 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* is respectfully requested.

It should also be pointed out that the rejection of Claims 1, 2, 5, 6, 13 and 14 under 35 U.S.C. §103(a) over *Gillon* in view of *Elgamal* is believed to be improper on the ground that a person skilled in the art would not have been motivated to combine *Gillon* and *Elgamal* in the manner specified in the Office Action.

Claims 1, 2, 5, 6, 13 and 14 are directed to providing communication protocol-independent security for data. Furthermore, Claims 1, 2, 5, 6, 13 and 14 require a step of encrypting data to be transmitted between first and second processes.

Elgamal is generally directed to an approach to encrypting and decrypting information transferred over a network between a client application and a server application. On the other hand, *Gillon* is directed to an approach for compressing a continuous, indistinct data stream and is completely unrelated to data security in general and more specifically, protecting data through the use of encryption. *Gillon* is completely devoid of any reference whatsoever to data security or protecting data using encryption. Therefore, it is respectfully submitted that one skilled in the art would not be motivated to combine *Gillon* and *Elgamal* in the manner specified in the Office Action since *Gillon* is completely unrelated to data security in general and more particularly, protecting data using encryption. Accordingly, it is respectfully submitted that the rejection of

Claims 1, 2, 5, 6, 13 and 14 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* is improper on the ground that a person skilled in the art would not have been motivated to combine the references in the manner specified in the Office Action.

REJECTIONS OF CLAIMS 3, 4, 7, 8, 15 AND 16 UNDER 35 U.S.C. §103(a)

Claims 3, 4, 7, 8, 15 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff et al., ("van Hoff")* U.S. Patent No. 5,761,421. It is respectfully submitted that Claims 3, 4, 7, 8, 15 and 16 are not unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff* for at least the following reason.

Van Hoff describes an approach for providing secure peer-to-peer communication between downloaded programs. The approach allows two programs obtained from the same security domain and executing on two different client computers to communicate securely. *Van Hoff* does not each or suggest the step of "encrypting data to be transmitted between the first and second processes, the encrypting of the data being independent of the at least one communication protocol supported by the first and second network nodes" as is required by Claims 3, 4, 7, 8, 15 and 16. There is no mention in *van Hoff* of using protocol-independent encryption to protect data.

Therefore, since neither *Gillon* nor *Elgamal* teach or suggest this step as previously described, it is respectfully submitted that Claims 3, 4, 7, 8, 15 and 16 are not unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff*. Therefore, the reconsideration and withdrawal of the rejection of Claims 3, 4, 7, 8, 15 and 17 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff* is respectfully requested.

REJECTION OF CLAIMS 9 AND 10 UNDER 35 U.S.C. §103(a)

Claims 9 and 10 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon*. It is respectfully submitted that Claims 9 and 10 are not unpatentable over *Elgamal* in view of *Gillon* for at least the following reasons.

CLAIM 9

Claim 9 recites a communication network providing communication protocol-independent secure communication between a first network node and a second network node wherein the first network node and the second network node each support at least one common communication protocol. The communication network recited in Claim 9 requires the following elements:

"a) a first process executing on the first network node, wherein the first process provides for the communication protocol-independent encryption of data;
b) a first stream which provides for the transfer of encrypted data between the first process and the communication channel;
c) a second process executing on the second network node; and
d) a second stream which provides for the transfer of encrypted data between the communication channel and the second process, wherein the second process also provides for the decryption of data which has been encrypted by the first process."

In particular, the communication network recited in Claim 9 requires " a first process executing on the first network node, wherein the first process provides for the communication protocol-independent encryption of data." As previously described with respect to Claim 1, neither *Elgamal* nor *Gillon* teach or suggest, alone or in combination, communication protocol-independent encryption of data. Therefore, it is respectfully submitted that Claim 9 is not unpatentable over *Elgamal* in view of *Gillon*. Accordingly, the reconsideration and withdrawal of the rejection of Claim 9 under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* is respectfully requested.

CLAIM 10

Claim 10 depends from Claim 9 and includes all of the limitations of Claim 9. Therefore, it is respectfully submitted that for the reasons stated herein in support of Claim 9, Claim 10 is not unpatentable over *Elgamal* in view of *Gillon*. Accordingly, the reconsideration and withdrawal of the rejection of Claim 10 under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* is respectfully requested.

REJECTION OF CLAIMS 11 AND 12 UNDER 35 U.S.C. §103(a)

Claims 11 and 12 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* and further in view of *van Hoff*. It is respectfully submitted that Claims 11 and 12 are not unpatentable over *Elgamal* in view of *Gillon* and further in view of *van Hoff* for at least the reasons provided hereinafter.

Claims 11 and 12 depend on Claim 9 and include all the limitations of Claim 9. As previously described herein with respect to Claim 1, *Elgamal* and *Gillon* do not teach or suggest, alone or in combination, performing communication protocol-independent encryption of data. Furthermore, as previously described herein with regard to Claims 3, 4, 7, 8, 15 and 16, *van Hoff* does not teach or suggest communication protocol-independent encryption of data.

Therefore, it is respectfully submitted that Claims 11 and 12 are not unpatentable over *Elgamal* in view of *Gillon* and further in view of *van Hoff* since none of these references, alone or in combination, teach or suggest communication protocol-independent encryption of data, as required by Claims 11 and 12. Accordingly, the reconsideration and withdrawal of the rejection of Claims 11 and 12 under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* and further in view of *van Hoff* is respectfully requested.

REJECTION OF CLAIM 17 UNDER 35 U.S.C. §103(a)

Claim 17 has been rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal*. It is respectfully submitted that Claim 17 is not unpatentable over *Gillon* in view of *Elgamal* for at least the reasons provided hereinafter. Claim 17 recites a method for providing communication protocol-independent security for data transmitted by a process executing on a network node. The method recited in Claim 17 requires the steps of:

"a) establishing a stream between the process and a communication channel;
b) encrypting data to be transmitted by the process, the encrypting of the data being independent of a communication protocol supported by the network node;
c) writing the encrypted data to the stream; and
d) causing the encrypted data to be transmitted from the network node to the communication channel."

Claim 17 addresses the problem of how to provide communication protocol-independent security for data transmitted by a process executing on a network node. Claim 17 solves this problem by encrypting data to be transmitted by the process independent of the communication protocol supported by the network node on which the process executes.

As previously described herein with respect to Claim 1, *Gillon* and *Elgamal*, do not teach or suggest, alone or in combination, encrypting data independent of a communication protocol which is required by Claim 17. Therefore, it is respectfully submitted that Claim 17 is not unpatentable over *Gillon* in view of *Elgamal*. Accordingly, the reconsideration and withdrawal of the rejection of Claim 17 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* is respectfully requested.

REJECTION OF CLAIMS 18 AND 19 UNDER 35 U.S.C. §103(a)

Claims 18 and 19 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff*. It is respectfully submitted that Claims 18 and 19 are not unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff* for at least the reasons provided hereinafter.

Claims 18 and 19 depend on Claim 17 and include all the limitations of Claim 17. Specifically, Claims 18 and 19 require the step of "encrypting data to be transmitted by the process, the encrypting of the data being independent of a communication protocol supported by the network node." As previously described with respect to Claim 11, 12 and 17, *Gillon*, *Elgamal* and *van Hoff* do not teach or suggest, alone or in combination, encrypting data independent of a communication protocol, as required by Claims 18 and 19. Therefore, it is respectfully submitted that Claims 18 and 19 are not unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff*. Accordingly, the reconsideration and withdrawal of the rejection of Claims 18 and 19 under 35 U.S.C. 103(a) as being unpatentable over *Gillon* in view of *Elgamal* and further in view of *van Hoff* is respectfully requested.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a notice of allowance is

respectfully requested. The Examiner is invited to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

If there are any additional charges, please charge them to our Deposit Account No. 50-0385.

Respectfully submitted,

McDERMOTT, WILL & EMERY

Edward A. Becker
Reg. No. 37,777

600 13th Street, N.W.
Washington, DC 20005-3096
(408) 271-2300 EAB:ccf
Date: April 12, 1999
Facsimile: (408) 271-2310

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231

on 4/12/99 by Clare C. Finney